Listing of Claims:

This listing of claims reflects all claim amendments and replaces all prior versions, and listings, of claims in the application. Material to be inserted is in **underline**, and material to be deleted is in ~~strikeout~~ or (if the deletion is of five or fewer consecutive characters or would be difficult to see) in double brackets [[ ]]. Any cancellations are without prejudice.

1. (Previously presented) A method for videoconferencing using Internet Protocol (IP), the method comprising the steps of:

installing a videoconferencing services switch at an access point to a service provider IP network;

at the switch, registering a plurality of subscribers for videoconferencing services, each subscriber including a plurality of endpoints;

receiving subscriber-specific settings to be applied to multiple videoconferencing calls from the plurality of endpoints associated with each subscriber;

storing the subscriber-specific settings at a location accessible to the switch; and

configuring the switch to connect calls from the plurality of endpoints at each subscriber based on the corresponding subscriber-specific settings.

2. (Original) The method of claim 1, wherein subscriber-specific settings include policies selected from the group consisting of outbound/inbound calling privileges, encryption policies, bandwidth policies, priority among users policies, participation privileges, inbound/outbound calling restrictions, time-of-day restrictions, audio or video restrictions.

3. (Original) The method of claim 1, wherein subscriber-specific settings include firewall settings.

4. (Original) The method of claim 1, wherein subscriber-specific settings include network address translation (NAT) settings.

5. (Previously presented) A method for use in videoconferencing, the method comprising:

installing a videoconferencing services switch on a service provider network at an access point configured to enable multiple enterprise subscribers to access a global packet-switched computer network to exchange data, including videoconferencing data and non-videoconferencing data, the videoconferencing services switch being configured to process videoconferencing data from multiple enterprise subscribers;

at the videoconferencing services switch, receiving a request for a videoconferencing call from an origination endpoint of one of the multiple enterprise subscribers;

connecting the videoconferencing call to a destination endpoint, the videoconferencing call having associated videoconferencing data; and

securing the videoconferencing call based on subscriber-specific security settings.

6. (Previously presented) The method of claim 5, wherein each enterprise subscriber includes an enterprise gateway positioned on the network between the access point and the origination endpoint, the method further comprising:

routing videoconferencing data from the enterprise gateway to videoconferencing services switch; and

routing non-videoconferencing data from the enterprise gateway around the videoconferencing services switch.

7. (Previously presented) The method of claim 6, wherein the videoconferencing data is routed to the videoconferencing services switch via a direct network connection from an enterprise router to the videoconferencing services switch.

8. (Previously presented) The method of claim 6, wherein the videoconferencing data is routed to the videoconferencing services service switch through an access point edge router.

9. (Original) The method of claim 8, wherein a firewall exists between the enterprise gateway and the video conferencing data is passed the firewall unexamined.

10. (Previously presented) The method of claim 9, wherein the videoconferencing data routed through the firewall is encrypted.

11. (Original) The method of claim 10, where the encryption is achieved using the IPSec protocols.

12. (Original) The method of claim 6, where the videoconferencing data is routed to the switch via a DSL network.

13. (Original) The method of claim 12, where the videoconferencing data is routed to the switch via PVC opened on the DSL network.

14. (Original) The method of claim 5, wherein the call is connected according to H.323 or SIP protocols.

15. (Original) The method of claim 5, wherein the security settings include firewall settings.

16. (Original) The method of claim 5, wherein the security settings includes NAT settings.

17. (Original) The method of claim 5, wherein subscriber-specific settings include policies selected from the group consisting of outbound/inbound calling privileges, encryption policies, bandwidth policies, priority among users policies, participation privileges, inbound/outbound calling restrictions, time-of-day restrictions, audio or

video restrictions.

18 – 52. (Canceled)

53. (Currently amended) The system of claim [[52]]54, wherein the enterprise video gateway includes an emulation module configured to emulate H.323/SIP call control and firewall functionality.

54. (Currently amended) ~~The system of claim 52,~~ A system for use in videoconferencing, the system comprising:

multiple enterprise subscriber networks, each enterprise subscriber network having one or more videoconferencing terminals;

a service provider network configured to enable users of the multiple enterprise subscriber networks to access a global computer network via an access point; and

a videoconferencing services switch positioned on the access point of the service provider network, the videoconferencing services switch being configured to process videoconferencing calls from terminals of each of the multiple enterprise subscriber networks, based on subscriber specific settings;

wherein a first enterprise subscriber network includes an enterprise video gateway; and

wherein the enterprise video gateway includes an encryption module configured to encrypt videoconferencing data sent between the videoconferencing services switch and the enterprise video gateway.

55. (Original) The system of claim 54, wherein the encryption module is configured to encrypt videoconferencing data using IP Security (IPSec) authentication and encryption.

56. (Currently amended) The system of claim [[52]]54, wherein the first enterprise subscriber network includes an enterprise router configured to route videoconferencing data to the videoconferencing services switch.

57. (Currently amended) The system of claim [[52]]54, further comprising, a direct network connection dedicated to video traffic linking the first enterprise subscriber network and the videoconferencing services switch.

58. (Currently amended) The system of claim [[52]]54, wherein the access point on the service provider network is a point of presence (POP).

59. (Original) The system of claim 58, wherein the service provider network includes an edge router configured to route videoconferencing traffic between the multiple subscriber networks and the videoconferencing services switch.

60. (Original) The system of claim 58, wherein the service provider network includes a core router configured to route videoconferencing traffic across a computer network backbone to a destination terminal in a remote zone.

61. (Currently amended) ~~The system of claim 52,~~ A system for use in videoconferencing, the system comprising:

multiple enterprise subscriber networks, each enterprise subscriber network having one or more videoconferencing terminals;

a service provider network configured to enable users of the multiple enterprise subscriber networks to access a global computer network via an access point; and

a videoconferencing services switch positioned on the access point of the service provider network, the videoconferencing services switch being configured to process videoconferencing calls from terminals of each of the multiple enterprise subscriber networks, based on subscriber specific settings;

wherein a first enterprise subscriber network includes an enterprise video gateway; and

wherein the videoconferencing services switch includes, (1) a virtual router configured to receive a request for a videoconferencing call from an origination terminal via the enterprise gateway, and (2) a call control module configured to perform call set-up operations, manage call data streams, and perform call tear down operations for the videoconferencing call, wherein the virtual router is configured to route call-related traffic between the origination terminal and the call control module.